Силабус освітнього компонента
Програма навчальної дисципліни

Інтернет речей та сервісів

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

Євсеєв Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 337, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 29 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 156 статті у закордонних виданнях та фахових виданнях України, з них 40 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів.

Детальніше про викладача на сайті кафедри

Погасій Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua
Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи

побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Інтернет речей та сервісів" є вибірковою навчальною дисципліною. Вивчення дисципліни сприяє підготовці фахівців, що володіють здатністю проектувати та розробляти розумні пристрої, що є частиною розумних систем чи інтелектуального середовища; формує стійкі знання та навички у студентів з розробки апаратних компонентів інтелектуальних систем IoT. Оволодіння програмою курсу сприяє виконанню студентами завдань з інших дисциплін, які передбачають наукові та практичні дослідження, щодо застосування результатів проектування систем IoT («Інтернет речей»). Засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами дослідження і проектування засобів Інтернету речей, що дасть можливість більш глибшого розуміння реалізації його основних функцій.

Мета та цілі дисципліни

Формування системи знань студентів в області Інтернет речей та цифрових технологій, та більш широкої категорії, яка називається цифровим перетворенням на базі яких дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких системи на виробництві та в науковій сфері. В дисципліні основний акцент робиться на розумінні фундаментальних концепцій і механізмів які лежать в основі функціонування Інтернет речей.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Організаційне забезпечення засобів інформації.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Історія інтернету речей.
Історія розвитку інтернету речей. Перспективи розвитку інтернету речей. Архітектура та ресурси сучасних операційних систем.
Тема 2. IoT платформи.
Платформа Linux Foundation.Пплатформа AggreGate. Платформа Everyware Cloud.
Тема 3. Прості та інтелектуальні сенсори.
Уточнення поняття "сенсор". Прості сенсори. Активні та пасивні сенсори. Сенсорно-комп'ютерні системи. Інтелектуальні сенсори. Класифікація інтелектуальних сенсорів.

Тема 4. Інтелектуальні акустичні сенсори. Електричні сенсори.
Фізичні основи роботи акустичних сенсорів. Приймачі акустичних сигналів.Інтелектуальні акустичні сенсори. Тонометри. Гідролокатори. Риборозшукові ехолоти. УЗ-сенсори відстані. Інтелектуальні портативні сенсори для УЗ досліджень. Физичні основи роботи електричних сенсорів. Резистивні сенсорі. Ємнісні та імпедансні сенсори.
Тема 5. Технології Інтернет речей.
Передача даних в архітектурі IIoT: MQTT.
Тема 6. Передача та обробка даних Інтернет речей.
Принцип роботи IoT. Зчитування інформації за допомогою датчиків. Передача даних від датчиків до хмарних сховищ. Обробка даних отриманих за допомогою датчиків. Передача даних на інтерфейс користувача. Основи HTTP. WEB API. Основи REST. Явне використання HTTP-методів. Відображення URI, аналогічних структурі каталогів. Технології та протоколи передачі даних на довгі відстані в IoT мережах:LoRaWAN, SigFox,. NB-IoT,. Weightless-P. Технології та протоколи передачі даних на короткі відстані в IoT мережах: Z-Wave, NFC, RFID, Bluetooth Low Energy, Wi-Fi HaLow. Протоколи для передачі повідомлень в IoT.
Тема 7. Сенсорні мережі.
Стандарти. Класифікація. Технології. Конструктивні особливості. Протоколи.
Тема 8. Технології обробки великих даних (Big Data).
Принципи роботи з великими даними. Технології і тенденції роботи з Big Data. Обробка і методи аналізу Big Data. Великі дані у промисловості. Алгоритми кластеризації Big Data. Проблеми опрацювання різнотипної інформації.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Packet Tracer - Розгортання та з'єднання пристроїв.
Тема 2. Створення простої домашньої мережі за допомогою Packet Tracer.
Тема 3. Отримання блимаючого індикатора за допомогою Blockly.
Тема 4. Packet Tracer. Додавання пристроїв IoT в роумний будинок.
Тема 5. Підключення та моніторинг пристроїв IoT.
Тема 6. Розумна кімната на базі Raspberry Pi і PL-App.
Тема 7. Основи роботи з Node-RED.
Тема 8. Вивчення протоколів IoT. Протокол MQTT.
Тема 9. Використання WEB API та Web-сокетів.
Тема 10. Вивчення основ роботи з хмарною платформою IBM Cloud.
Тема 11. Вивчення основ роботи з хмарними сервісами для збереження об’єктів.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт та заліку.

Література та навчальні матеріали

Основна література:

1. Дэвид Роуз, Дэвид Роуз (David Rose), Будущее вещей. Как сказка и фантастика становятся реальностью, ISBN: 978-5-91671-394-7, 2015.
2. В. А. Петин, Arduino и Raspberry Pi в проектах Internet of Things, ISBN: 978- 5-9775-3646-2, 2016, 320с.
3. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.

4. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P.
5. Cuno Pfister, Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud (Make: Projects) 1st Edition, ASIN: B00COVJUGI, 2011, 194 P.
6. Erik Brynjolfsson and Andrew McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies 1st Edition, ASIN: B00D97HPQI, 2014, 320 P.
7. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P.
8. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
9. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с.

Додаткова література :

1 Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.
2. Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.
3. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
4. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
5. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	28.08.2023		Завідувач кафедри Сергій ЄВСЕЄВ
	28.08.2023		Гарант ОП Олександр МІЛОВ